SECURE EMAIL AGREEMENT

The Los Angeles County Department of Mental Health (LAC-DMH) is providing a secure email solution for its workforce to communicate all confidential data, including but not limited to Protected Health Information (PHI), while maintaining the confidentiality of information as required by Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other applicable federal, State, local laws, or regulations related to confidentiality.

As a member of the LAC-DMH workforce, I acknowledge and agree to be bound by all the terms, conditions, and policies of this Agreement, including any future amendments. I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including suspension, discharge, cancellation of contracts, and the possibility of civil and/or criminal penalties. I further understand that I must review and follow DMH Policy No. 557.02, Appropriate Use of Email for Transmitting PHI and/or Confidential Data, as well as DMH Policy No. 506.02, Privacy Sanctions and all other HIPAA Privacy and Security Policies.

As an authorized DMH workforce member, I agree to abide by the following:

1. I will exercise extreme care to ensure email with PHI/Confidential Data is sent to the recipient's correct email address.

2. I will email only the minimum necessary PHI to protect the client's privacy and to minimize risk of unauthorized use of PHI.

3. I will email only PHI that is factual and based on sufficient information gathered and supported by documentation found in the Clinical Record. Email will not include opinions or determinations of psychological fitness or capacity.

4. I will not send email communications containing PHI/Confidential Data to mailing distribution lists or shared email accounts.

5. I will not include any PHI/Confidential Data in the 'Subject Line'.

6. I will not text PHI/Confidential Data. If I receive a text message that includes PHI/Confidential Data I will respond to the sender via other means of communication (e.g., telephone or mail) with instructions to delete the text message immediately.

7. I will not send PHI/Confidential Data by non-County email systems (e.g., Yahoo-Mail, Hotmail, G-Mail, AOL-Mail, etc.).

8. All email to clients is considered PHI and must be encrypted. I am aware of the standards that must be followed which permit LAC-DMH workforce members to use the Secure Email as a method of communication with clients for specific and limited purposes (e.g., scheduling appointments, sending reminders about appointments and treatment instructions).

9. I will insert the word "[secure]", including the brackets, at the front of the subject line on all emails containing PHI/Confidential Data in order to encrypt the email.

The signed copy of this agreement must be maintained in workforce member's facility personnel folder.

10. I will print the final email communication and I will include attachments containing PHI from an email string (both received and sent) and ensure that it is placed in the client's clinical record in the "Correspondence" section or in a non-open PHI file. Complete a Progress Note that references the attached email.

    a. Email containing PHI that is administrative in nature will be stored in administrative files and not in the Clinical Record.

    b. Clinical and administrative related documents containing PHI or confidential data are subject to the same security requirements.

11. I will delete all email containing PHI from "Inbox", "Sent", "Deleted" and any other mailbox folders once they have been printed.

12. I will follow the breach notification procedure as outlined in DMH Policy No. 506.03, "Responding to Breach of Protected Health Information," in the event that an email containing PHI is wrongly sent or misdirected.

13. I will obtain approval before sending any email containing PHI for 100 clients to 499 clients from a program manager or higher level manager; any email containing PHI for 500 clients or more I will obtain approval from the program manager AND the LAC-DMH Information Security Officer or designee.

14. I will comply with DMH Policy No. 506.02, Privacy Sanctions, and other HIPAA privacy and security policies that are accessible on the LAC-DMH Intranet web site.

I certify that the agreement and policies listed above have been reviewed with me as of the date indicated below. I understand the provisions of the agreement; I have completed the required training and have read this agreement form.

Employee Name (print)	Employee Signature	Date

As a LAC-DMH employee performing in a management or supervisory capacity, I acknowledge that I am responsible for:

Ensuring that employees under my authority, who are authorized to send email communications containing PHI or Confidential Data, sign and comply with this Secure Email Agreement

Supervisor Name (print)	Supervisor Signature	Date

Program Manager/Head Name (print)	Program Manager/Head Signature	Date

The signed copy of this agreement must be maintained in workforce member's facility personnel folder.